IPPF
International Professional Practices Framework

Internal Audit and Fraud:

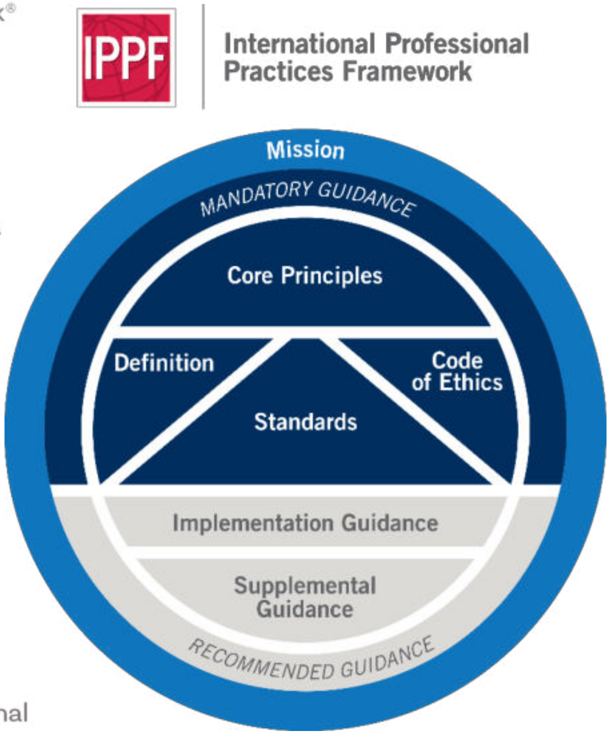
Assessing Fraud Risk Governance and Management at the Organizational Level, 2nd Edition

Supplemental Guidance | **Practice Guide**

The Institute of
Internal Auditors

About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA for internal audit professionals worldwide.



Mandatory Guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- International Standards for the Professional Practice of Internal Auditing.

Recommended Guidance includes Implementation and Supplemental Guidance. Implementation Guidance is designed to help internal auditors understand how to apply and conform with the requirements of Mandatory Guidance.

About Supplemental Guidance

Supplemental Guidance provides additional information, advice, and best practices for providing internal audit services. It supports the *Standards* by addressing topical areas and sector-specific issues in more detail than Implementation Guidance and is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides, a type of Supplemental Guidance, provide detailed approaches, step-by-step processes, and examples intended to support all internal auditors. Select Practice Guides focus on:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.theiia.org.

Contents

Executive Summary **2**

Introduction: Understanding and Assessing Fraud Risk **3**

Fraud: Considerations for the Internal Auditor 3

IPPF Standards on Fraud 4

Fraud Risk Governance and Management **6**

Board Roles 6

Management Roles 7

Internal Audit: Third Line Roles 8

Effective Fraud Risk Management Program: Using a Framework **11**

COSO Framework for Fraud Risk Management 11

Providing Assurance on Organizationwide Fraud Risk Governance and Management **14**

Coordination and Reliance 14

Purpose, Authority, and Responsibility of the Internal Audit Activity 14

Maintaining Objectivity and Independence 16

Assessing Organizationwide Fraud Risk Governance and Management 17

Appendix A. Related IIA Standards and Guidance **22**

Appendix B. Glossary **23**

Appendix C. References and Additional Reading **25**

Acknowledgements **26**

Executive Summary

The purpose of this practice guide is to increase the internal auditor's awareness of fraud risk, including the role the internal audit activity can play, and provide guidance on how to perform a fraud risk assessment at an organizational level. The IPPF requires internal auditors to consider the risk of fraud in their work. The internal audit activity must evaluate the potential for fraud and how the organization manages fraud risk, as per Standard 2120.A2.

Implementation of this guide is intended to:

- Increase the internal auditor's awareness and understanding of organizational fraud risk governance and management.
- Explain the various roles responsible for preventing, detecting, assessing, and investigating fraud at the organizational level and how they interact using The IIA's position paper, The Three Lines Model.[1]
- Describe the purpose and benefits of utilizing a fraud risk management framework, with specific reference to COSO's *Fraud Risk Management Guide*.
- Explain the role the internal audit activity may play in the organization's fraud risk management program.
- Identify the requirements for the internal audit activity to provide assurance on organizationwide fraud risk governance and management. These include:
    - Evaluating structures and processes for fraud risk governance.
    - Performing an organizationwide assessment of fraud risks.
    - Evaluating the design of the fraud risk management program.
    - Evaluating operationalization of the fraud risk management program.
    - Communicating results and assurance to senior management and the board.

This second edition practice guide supersedes Practice Guide "Internal Auditing and Fraud" originally issued in 2009.

Note: Assessing fraud risks relevant to specific auditable areas and processes during individual engagements is not discussed. That topic appears in Practice Guide "Engagement Planning: Assessing Fraud Risks."

[1] The IIA, "The Three Lines Model," 2020. https://www.theiia.org/en/content/articles/global-knowledge-brief/2020/july/the-iias-three-lines-model/.

Introduction: Understanding and Assessing Fraud Risk

Fraud: Considerations for the Internal Auditor

According to COSO's *Fraud Risk Management Guide*, "fraud deterrence is a process of eliminating factors that may cause fraud to occur." Fraud risks may be internal or external to the organization and include collusion, under- or over-reporting, misappropriation of assets or data, misrepresentation, falsification of documents, and destruction of records.

The internal audit activity contributes to fraud deterrence by providing assurance on the adequacy and effectiveness of fraud risk **governance** and management, and advising on opportunities for improvement. An assessment at an organizationwide level of fraud risk governance and management can be made by aggregating findings from multiple engagements at a more granular level or making a holistic review.

To be effective in this role, internal auditors need a clear understanding of:

- The nature and characteristics of fraud.
- The potential for fraud risk within their organization.
- Effective strategies for fraud risk governance and management.
- Roles and responsibilities regarding fraud risk.
- How to provide senior management and the **board** with an opinion on fraud risk governance and management overall.

Definitions of fraud vary. In some cases, fraud is defined as a part of regulation, creating complexities for organizations that span multiple jurisdictions. Given the range of different kinds of fraud and how these may impact a particular organization at a particular time, internal

Definition

The glossary in the 2017 edition of the IPPF defines **fraud** as "any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."

The related concept of **corruption** is defined as "the use of power, money, or favors by people in positions of authority or contacts in their network for illegitimate private gain." (Practice Guide "Auditing Anti-corruption Activities").

Note

Terms in **bold** are defined in Appendix B.

auditors need to use their knowledge and skills to ensure their fraud risk assessment is timely and relevant.

However, there are certain important characteristics of fraud for the internal auditor to note. These include:

- Pressure or incentive.
- Perceived opportunity.
- Rationalization.[2]

Acts of fraud are deliberate. Unlike cases of negligence, perpetrators of fraud intentionally seek to take advantage of circumstances by exploiting weaknesses in **controls***, either because they are under duress or for personal gain. Typically, they attempt to justify their actions – to themselves and possibly to others – as somehow legitimate or deserved.

Organizations and their internal auditors need to be mindful of *fraud risk* (when there is potential for fraud), *fraud schemes* (when fraud is being planned), and *fraud events* (when fraud has been perpetrated).

IPPF Standards on Fraud

In the IPPF, fraud is mentioned as an attribute of internal audit proficiency (Standard 1210 – Proficiency) and **due professional care** (Standard 1220 – Due Professional Care). Standard 1210.A2 requires internal auditors to "have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud." According to Standard 1220.A1, the probability of fraud must be considered as part of due professional care during an assurance engagement.

When evaluating the effectiveness of an organization's risk management processes overall (Standard 2120 – Risk Management), the internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk (Standard 2120.A2). This guide describes how to evaluate fraud risk governance and management in the organization as a whole. It discusses the relevant roles and responsibilities of the internal audit activity and the **chief audit executive** (CAE).

Essential Resources

Practice Guide "Engagement Planning: Assessing Fraud Risks" introduces basic fraud information, such as an explanation of the elements of Cressey's Fraud Triangle. The guide describes types of fraud, provides examples of potential fraud indicators, and details the process of identifying and assessing fraud risk.

Practice Guide "Auditing Anti-corruption Activities" discusses the role of internal auditors in anti-corruption efforts.

[2] Donald Cressey. Other People's Money: A Study in the Social Psychology of Embezzlement (Glencoe, IL: Free Press, 1953).

Additionally, the CAE must report periodically to senior management and the board on significant risks and any control issues, which explicitly includes fraud risks (Standard 2060 – Reporting to Senior Management and the Board). When planning individual engagements and developing the engagement objectives, internal auditors must consider the probability of fraud (Standard 2210.A2). This type of risk assessment is detailed in the Practice Guide "Engagement Planning: Assessing Fraud Risks."

Organizational Considerations

There is no "one size fits all" for fraud risk management. How fraud risks are defined, recognized, managed, and mitigated within an organization depends on factors such as its:

- Sector, industry, and location.
- Size, organizational structure, and strategic objectives.
- Structures and systems for governance, risk management, and internal control.
- Culture, tone, and values.
- Management information systems and use of technology.
- Operating environment, including regulatory oversight and legislation (local, regional, national, and international).

The identification, assessment, and prioritization of fraud risks, schemes, and events, together with the organization's response to these, should be determined by these characteristics. Management and the board must identify the level of fraud risk they are willing to accept (that is, the organization's **risk appetite**) and weigh the cost of controlling risks against the benefits of mitigating or eliminating them.

Accordingly, to provide assurance and advice on the adequacy and effectiveness of fraud risk governance and management, internal auditors must develop and maintain a strong understanding of all aspects of the organization. Key to the success of tackling fraud risk is the appropriate allocation of roles, responsibilities, and resources, and the Three Lines Model provides an effective tool to help with this.

Fraud Risk Governance and Management

Addressing fraud risk is a shared responsibility for everyone, starting with the board and extending throughout the organization. Formal arrangements for managing fraud risk may also include external consultants, providers of assurance, and other fraud experts.

The IIA's position paper, The Three Lines Model, provides a flexible tool to help establish clear roles, structures, and interrelationships for governance and management to ensure coherence, and it can be applied to organizational arrangements for addressing fraud risk. The model emphasizes the importance of:

- Clear and consistent tone from the top.
- Collaboration across the organization.
- The **independence** of the internal audit activity.

Board Roles

The board has ultimate responsibility for effective fraud risk governance and helps set the appropriate tone at the top. Working with senior management, it must create the right expectations for ethical behavior and set the appetite for fraud risk. The board may appoint one of its members or an executive leader to champion fraud risk awareness and help coordinate activities.

The board should ensure there is an appropriate fraud risk management framework and program in place. To achieve this, it monitors and evaluates management's antifraud activities, including the identification and assessment of fraud risks, implementation of antifraud measures, and ongoing assessment of the effectiveness of the fraud risk program. It may request reports from management and the internal audit activity. The CAE will provide periodic reports to senior management and the board on internal audit's assessment of fraud risk.

Audit Committee

A board may establish a separate audit committee to oversee the internal audit activity. In such cases, the board may assign roles to the audit committee to assist in the monitoring and oversight of fraud risk, including controls to prevent or detect fraud by management. In this case, the audit committee is responsible for overseeing senior management's compliance with appropriate financial reporting and for preventing override of controls or other inappropriate influence over the reporting process.

Management Roles

Management is charged by the board with achieving the objectives of the organization and has the primary responsibility for monitoring and controlling processes to prevent, deter, detect, and recover from fraud.

Management is responsible for establishing and maintaining an effective internal control system at a reasonable cost, including considering the use of technology to assist in fraud risk management activities. Management oversees the activities of employees and typically does so by implementing and monitoring processes and internal controls, especially those related to day-to-day operations. In addition, management assesses the vulnerability of the entity to fraudulent activity.

The allocation of managerial roles varies by organization. In some cases, a separate resource is allocated to provide additional expertise and oversight regarding fraud risk. Regardless of the structure, these roles remain within the overall responsibility of management.

Management: First Line Roles

In their day-to-day activities, those with first line roles are expected to implement and monitor fraud risk and controls. This includes following procedures for escalation if fraud is suspected. If managers with first line roles have the skills to do so, they may be responsible for supporting the identification and assessment of fraud risks within their business unit. They may also be responsible for helping design the policies, procedures, and tools for fraud risk assessment, analysis, controls, and monitoring, including the use of data analytics to prevent and detect fraud. Whether or not they assist with the risk assessment, managers in these roles should be aware of, and responsive to, the risks in the area for which they are responsible.

Management: Second Line Roles

Where separate specialist second line functions are established, they generally lead fraud risk management activities while working closely with senior management.

The nature and types of these functions are dependent on many factors, including industry, organizational maturity, and size. They ensure properly designed processes and controls to mitigate fraud risks are in place and operating effectively under the auspices of those with first line roles. Specific fraud risk functions may include loss prevention managers, fraud investigators, financial crimes specialists, and fraud operation personnel.

Organizational alignment of such functions varies but they operate more effectively when senior management and internal audit work closely with legal counsel and other second line functions. This includes developing, maintaining, and implementing a robust investigation process. Laws, regulations, policies, materiality, and other considerations help determine communication needs and when to involve the board, external auditors, law enforcement, or other authorities.

Smaller organizations with limited resources may choose to cosource or outsource fraud risk expertise or rely on internal audit to take a more active role in fraud risk management activities.

Participation by the internal audit activity depends on its charter, internal auditor proficiency, and resource prioritization. Care must be taken to ensure appropriate independence and **objectivity**.

Internal Audit: Third Line Roles

The internal audit activity provides assurance to the board and senior management on how effectively the organization assesses and manages its fraud risks. This would include consideration of the overall coherence of fraud risk management activities and their alignment with organizational strategy and operations.

In all matters, internal auditors should be directed by their commitment to due professional care and to upholding the Code of Ethics and the Rules of Conduct relating to integrity, objectivity, confidentiality, and competency. Not only should they demonstrate the utmost integrity in their behavior, they should also lead by example. Awareness of the potential for fraud should inform engagement planning, delivery, and communication.

Specific roles may include contributing to policy development and fraud training, and supporting investigations. However, the internal audit activity's role in the governance and management of fraud risks should be clearly stated in its charter and reflected in its policies and procedures. This is to ensure senior management and the board understand and agree to the role and recognize any safeguards to help maintain independence of the internal audit activity and objectivity of internal auditors.

Through individual engagements and as part of organizationwide risk governance and management audits, internal auditors provide independent and objective assurance over all aspects of fraud risk that are material or significant. Internal auditors gather insights about the organization, its control environment, and its fraud risk management culture through every audit engagement.

Figure 1 illustrates organizational roles and responsibilities for fraud risk governance and managementusing the Three Lines Model.

Figure 1: Fraud Risk Governance and Management – Organizational Roles and Responsibilities

Organizational Component	Primary Roles	Fraud Risk Roles
1. Board, audit committee	• Highest decision-making authority within the organization responsible for governance. • Comprises a majority of independent directors. • Ultimately accountable to stakeholders for oversight of all activities and results.	• Ensuring effective fraud risk governance, including an antifraud culture and tone at the top, working closely with senior management. • Defining and demonstrating ethical principles for fraud. • Obtaining outside fraud expertise when needed. • Setting risk appetite for fraud. • Overseeing, monitoring, and evaluating the execution of fraud risk management. • Ensuring an appropriate fraud risk framework and program. • Establishing an appropriate committee structure and resource to discharge responsibility for fraud risk oversight. • Considering reports from management, internal audit, and other advisors on fraud.
2. Management	• Authorized by the board to apply resources and execute decisions, including managing risk, to achieve organizational objectives in an effective, efficient, ethical, and sustainable manner.	• Leading fraud risk management to prevent, deter, detect, and recover from fraudulent acts. • Adopting an appropriate fraud risk management framework. • Setting antifraud tone consistent with the board. • Overseeing staff activities and enforcing antifraud policies. • Identifying and prioritizing fraud risk. • Establishing and maintaining a fraud risk communication strategy and providing fraud training. • Enabling whistleblowing without prejudice. • Ensuring follow up on the findings and recommendations of internal audit related to control weaknesses and opportunities for improvement to fraud risk management.
2.1 Management – first line roles	• Responsible for actions to achieve the core purpose of the organization through the provision of goods and services to clients and maintaining the operations that underpin this.	• Planning and participating in fraud risk assessment activities. • Implementing, monitoring, and maintaining antifraud controls, including communications strategy. • Promoting employee awareness of fraud risk and controls. • Escalating fraud risk events in accordance with policy and procedures. • Supporting investigations into fraud schemes and events. • Applying corrective actions and disciplinary procedures in response to fraud events.
2.2 Management – second line roles	• Responsible for providing additional expertise and oversight in the management of risk. Examples of specialist second line roles and functions include: risk management; enterprise risk management; compliance; legal counsel; fraud investigators; loss	• Designing policies and procedures to inform fraud risk management, including implementation of control activities. • Implementing remedial actions to address weaknesses in policies and procedures for fraud risk management. • Analyzing conformance with, and the effectiveness of, fraud risk control activities. • Maintaining active monitoring of the internal and external operating environments for changes to fraud risk profile, including new and emerging fraud risks. • Leading the investigation of fraud schemes and events. • Providing fraud risk training.

	prevention managers; and security.	• Providing reports and other support to senior management and the board on aspects of fraud risk management.
3. Third line roles- internal audit	• Independent function without management responsibilities or interference, led by the chief audit executive, accountable to the board either directly or via an independent audit committee.	• Reporting to senior management and the board on the adequacy and effectiveness of fraud risk governance and management at an engagement and organizationwide level. • Conducting periodic and ad hoc assessments of fraud risk management programs utilizing a suitable framework as appropriate to inform their approach. • Providing insight and advice to senior management and the board on opportunities for improvement to fraud risk management. • Contributing to organizational fraud risk awareness and training at the request of senior management.

Effective Fraud Risk Management Program: Using a Framework

Effective fraud risk management requires the implementation of a comprehensive, holistic, and systematic program. This entails appropriate policies, tools, training, and other antifraud control activities and a commitment at all levels to communicating and enforcing an antifraud culture. To develop, maintain, and review such a program, organizations should use a suitable framework aligned with their internal control environment and broader risk management activities. The use of a framework helps organizations:

- Establish a fraud risk management program in a methodical way to identify, assess, manage, communicate, and monitor fraud risk.
- Ensure consistency in approach in implementing a fraud risk management program, especially in large and complex organizations where standardization may be difficult.
- Determine whether the fraud risk management program is properly designed and operating effectively.

The board and senior management may choose to develop their own framework or to adopt and adapt an existing model (such as COSO's *Fraud Risk Management Guide*) to fit their organization. A relevant framework can also inform the internal auditor's assessment methodology, even if management has not explicitly adopted it.

COSO Framework for Fraud Risk Management

Principle 8 of COSO's 2013 *Internal Control – Integrated Framework* requires that organizations consider "the potential for fraud in assessing risks to the achievement of objectives." COSO's *Fraud Risk Management Guide* supplements this framework by providing information about performing a fraud risk assessment as well as guidance on establishing an overall fraud risk management program.

Figure 2 illustrates how the COSO model uses the five components of internal control as the basis for establishing five fraud risk management principles. From these principles, organizations can develop a program for managing fraud risk to fit their needs. The fraud risk management program will enable the organization to establish:

- A robust control environment.
- Reliable risk activities that manage fraud within the appetites set by senior management and the board.
- Effective preventive, detective, and corrective controls for fraud risk.
- A ready flow of information to support fraud risk management activities.

- A means for monitoring, evaluating, and making continuous improvements to the program.

Figure 2: COSO Internal Control Components and Fraud Risk Management Principles: Guide for Internal Auditors

Fraud Risk Management Framework		Fraud Risk Management Program
Internal Control Component	Fraud Risk Management Principle	Example Activities
1. Control Environment	Fraud Risk Governance – The organization establishes and communicates a fraud risk management program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.	Sound and transparent antifraud culture, governance processes, and control environment, including: • Independent oversight of fraud risk management by board or audit committee. • Strong antifraud tone at the top. • Commitment to swift action. • Codes of ethics and conduct. • Clearly defined management roles for fraud (including implementation of controls). • Antifraud policies and procedures, including ethical behavior and remedies for noncompliance. • Processes for identifying, investigating, and prosecuting fraud.
2. Risk Assessment	Fraud Risk Assessment – The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assesses their likelihood and significance, evaluates existing fraud control activities, and implements actions to mitigate residual fraud risks.	Thorough fraud risk assessments conducted periodically, including: • Self-assessments by management. • Third party assessments. • Internal audit-led or -assisted assessments. • Development of key risk indicators (KRIs). • Identification and monitoring of red flags for fraud risk.
3. Control Activities	Fraud Control Activity – The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.	Well-documented fraud preventive and detective control activities, such as: • User IDs and authentication. • User provisioning and deprovisioning. • Variance analysis and proactive data analytics. • Account reconciliations. • Fraud awareness training for all employees. • Mandatory vacations and job rotations to reduce the potential for individuals to cover up fraud schemes. • Antifraud hotline and anonymous surveys. • Whistleblower protection. • Periodic physical counts. • Physical security and surveillance. • Continuous and ad hoc management reviews and audits, including surprise audits.
4. Information and Communication	Fraud Investigation and Corrective Action – The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action	Systems for pre-planning, investigation, and corrective action processes: • Fraud risk communication strategy, including procedures for escalation and evaluation of potential and actual fraud events. • Control activity monitoring. • Cyclical review ("prompt, competent, and confidential," COSO).

	to address fraud appropriately and in a timely manner.	• Investigations of fraud and misconduct. • Root cause analysis. • Prompt resolution of noncompliance. • Disciplinary action as required.
5. Monitoring	Fraud Risk Management Monitoring Activities – The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates fraud risk management program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.	Systems for monitoring and evaluating the fraud risk management program overall integrated into routine business processes: • Periodic and ad hoc holistic assessments of fraud risk management program, including reports by the CAE to senior management and the board. • Management responsiveness to internal audit findings from ongoing and periodic evaluations and other reviews. • Timely resolution of weaknesses in the fraud risk management program.

Whistleblowers are integral to fraud deterrence and detection. Tip-offs are the most common method of detection, and an anonymous, well-managed, and confidential reporting system may deter many fraud schemes from ever happening. Such a system may include a hotline, webline, email, mobile app, and a paper-based mailbox. Whistleblowers' suspicions of fraud should be reported to management, a fraud investigation unit, a member of the board, internal audit, or other suitable recipient. Processes should be in place to ensure these are investigated promptly and escalated accordingly.

Providing Assurance on Organizationwide Fraud Risk Governance and Management

Coordination and Reliance

Assurance on fraud risk management comes from multiple sources, including:

- Management, in the form of reports, forecasts, and attestations to the board.
- Specialist second line functions, including loss prevention and fraud investigation.
- External providers of assurance, such as external auditors, inspectors, and consultants.
- The internal audit activity.

The Three Lines Model emphasizes the importance of collaboration among internal functions to ensure organizational coherence. Coordination is a role the internal audit activity is well-positioned to play through assurance mapping and close cooperation with other assurance providers. In accordance with Standard 2050 – Coordination and Reliance, the CAE should work with other assurance providers and share information to avoid duplication.

Joint planning between internal audit and management, including any specialist second line functions with oversight of aspects of fraud risk management, is also important. Some organizations have explicit protocols for cooperation in fraud risk management and investigations.

Audit planning and delivery are more effective when undertaken in collaboration with managers with first and second line roles who have the knowledge, skills, and expertise needed to support fraud risk assessment and analysis and to evaluate antifraud controls. The audit plan should be reviewed regularly to reflect the results of engagements as well as updated risk assessments and any actual fraud occurrences. When working with others, however, the CAE should consider the reliability of their work, taking account of proficiency, methodology, and level of independence. The CAE is responsible and accountable for ensuring adequate support for conclusions and opinions reached by the internal audit activity.

Purpose, Authority, and Responsibility of the Internal Audit Activity

The internal audit charter must formally define the purpose, authority, and responsibility of the internal audit activity, as required by Standard 1000 – Purpose, Authority, and Responsibility. The ability to provide effective assurance regarding fraud risk is dependent on two key factors:

- The independence of the internal audit activity.
- The objectivity, proficiency, and due professional care of internal auditors.

Independence of the Internal Audit Activity

Organizational independence of the internal audit activity is secured through having an "access all areas" mandate in the audit charter, accountability to the board (directly or via an audit committee), and freedom from the responsibilities of, and interference by, management. Interference from management includes attempts to alter or hide findings or to restrict access to resources or the scope of investigations. Management interference with a fraud assurance engagement may itself be an indicator of potential fraud and an attempt to cover it up. If the CAE suspects or has identified fraud by members of senior management, tactful and confidential communication with the board may be necessary in order not to jeopardize an investigation by tipping off the perpetrator.

Objectivity, Proficiency, and Due Professional Care of Internal Auditors

When providing assurance over fraud risk governance and management, internal auditors are expected to exercise objectivity – an impartial, unbiased attitude that avoids any conflict of interest. Internal auditor objectivity relies on adherence to professional standards and a code of ethics, proficiency, the exercise of due professional care, appropriate supervision and quality assurance arrangements, and the application of **professional skepticism.**

Internal auditors are required to have sufficient knowledge to evaluate the risk of fraud and how the organization manages fraud risk. However, they are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud, as per Standard 1210 – Proficiency. The CAE should coordinate with other assurance providers, such as legal and compliance, to evaluate the depth and breadth of expertise needed to handle fraud occurrences.

Internal auditors and the CAE are well-positioned to assess and advise on fraud risks and controls and the overall fraud risk management program because they have particular expertise and a broad view of the organization.

Internal auditors' roles in fraud risk could include:

- Support for investigations of suspected fraud.
- Root cause analysis.
- Control improvement recommendations.
- Monitoring of a reporting/whistleblower hotline.
- The disposition of (or following through with) fraud cases.
- Contributing to ethics training sessions.

Sometimes they are asked to assist in, or possibly lead, fraud investigations or to assume responsibility for implementing antifraud controls and more. This occurs especially in circumstances where:

- The organization has limited resources.
- The organization's risk management and governance are not mature.
- New compliance initiatives are introduced.

However, this poses potential threats to the independence of the internal audit activity and the objectivity of internal auditors due to a real or perceived **conflict of interest**. In accordance with Standard 1100 – Independence and Objectivity, threats to independence and to objectivity must be managed at the individual auditor, engagement, functional, and organizational levels.

The CAE has a responsibility to ensure the internal audit activity has or obtains the knowledge, skills, and other competencies needed to perform its responsibilities, including providing assurance over fraud risk. The skills needed for conducting fraud investigations, for example, are different from those required for the regular duties of an internal auditor, and include an understanding of the risks inherent in the process itself, such as the possibility of evidence being tampered with or destroyed. The organization may set requirements for specific roles, including certifications, designations, and training. If unavailable within the team, the CAE must obtain the necessary expertise through other means, such as cosourcing or outsourcing the work or by hiring fraud and/or legal experts.

Maintaining Objectivity and Independence

Internal auditors routinely monitor, assess, analyze, evaluate, and provide independent and objective assurance on the adequacy and effectiveness of all aspects of fraud risk management. They may also act in an advisory capacity in helping management develop, implement, and improve fraud risk management. However, if the internal audit activity is expected to provide independent assurance, internal auditors should not assume responsibility for managing fraud risks, including deciding, implementing, enforcing, and being accountable for aspects of the program.

Therefore, where internal auditors are acting in an advisory capacity, various safeguards are needed. This also applies when the CAE assumes roles outside of internal auditing, in accordance with Standard 1112 – Chief Audit Executive Roles Beyond Internal Auditing. Examples of safeguards include clear statements of responsibility in the internal audit charter, well-documented audit policies and procedures, a declaration of any potential **impairment**s to the board, and the use of an independent source to provide assurance over work where an internal auditor has played a significant advisory role within the previous 12 months, as per Standard 1130 – Impairments to Independence and Objectivity.

Instances where safeguards should be considered include:

- Designing antifraud controls, including policies and procedures.
- Advising on fraud investigations.
- Assisting in the development of disciplinary procedures for fraudsters.
- Monitoring and reporting fraud tip-offs from a whistleblower hotline.

Instances where independent assurance from another source will be required include:

- Selecting a fraud risk framework for implementation by management.
- Implementing antifraud controls.
- Leading and determining the outcome of a fraud risk investigation.
- Enforcing fraud policies and procedures.

Assessing Organizationwide Fraud Risk Governance and Management

To provide organizationwide assurance on fraud risk governance and management, internal auditors will need to assess the adequacy and effectiveness of:

- Fraud risk governance structures and processes.
- The fraud risk management program (using a suitable model such as the COSO *Fraud Risk Management Guide*).
- Management's fraud control and monitoring activity.

In doing so, internal auditors may draw upon knowledge and understanding from previous engagements in which significant fraud risks were considered. Internal auditors have a continual presence in the organization that provides them with a cumulative understanding of the organization and its control systems. In addition, as part of their review, internal auditors should undertake an organizationwide fraud risk assessment, working with those with first and second line roles while maintaining independence and objectivity.

Internal auditors may conduct proactive auditing to search for fraudulent acts such as the misappropriation of assets and the misrepresentation of information. For this they may use computer-assisted audit techniques, such as continuous auditing, data mining, and data analytics. Internal auditors may also employ analytical and other procedures to find unusual items and perform detailed analyses of high-risk accounts and transactions to identify potential fraud.

Internal Audit's Organizationwide Fraud Risk Assessment Process

While management is responsible for operationalizing fraud risk management, the internal audit activity should lead the assessment of fraud risk with inputs from management. It should discuss the results with responsible managers and in some cases may be expected to share its findings with external auditors, depending upon laws and regulations, or for other reasons.

Figure 3 illustrates appropriate steps for the internal audit activity to complete its assessment of fraud risks, utilizing components 10-14 of COSO's *Enterprise Risk Management – Integrating Strategy and Performance*, 2017 as a structure.

Figure 3: Internal Audit Activity's Organizationwide Fraud Risk Assessment

COSO Components and Principles 10-14	Internal Audit's Fraud Risk Assessment Process
10. Identifies Risk *The organization identifies risk that impacts the performance of strategy and business objectives.*	Identify potential for fraud in the context of organizational objectives and operations by utilizing: • Checklists. • Previously completed assessments (such as risk assessments completed by management and business units, internal audit, and other providers of assurance and consultants). • Fact-finding meetings with individuals and groups responsible for fraud risk activities.

	• Interviews, surveys, brainstorming sessions, and focus groups with stakeholders across the organization at all levels.
11. Assesses Severity of Risk *The organization assesses the severity of risk.*	Assess fraud risk severity by: • Identifying relevant fraud factors and potential fraud schemes. • Applying appropriate criteria (including measures for likelihood, impact, velocity, etc., consistent with organizational approaches for risk evaluation).
12. Prioritizes Risks *The organization prioritizes risks as a basis for selecting responses to risks.*	Analyze and evaluate fraud risks and prioritize accordingly in the context of organizational objectives.
13. Implements Risk Responses *The organization identifies and selects risk responses.*	Review organizational fraud risk responses by: • Mapping, or reviewing existing maps, of processes, and existing controls related to each potential fraud scheme. • Assessing residual risk and identifying assurance priorities.
14. Develops Portfolio View *The organization develops and evaluates a portfolio view of risk.*	Consider the interrelationships among fraud risks and the impact of other risks on the potential for fraud. Factors may include: • Restructuring, expansion, consolidation, mergers, and acquisitions. • Changes to roles and responsibilities. • Staff turnover, absences, and shortages. • Arrangements for recognition, reward, promotion, and compensation. • Economic conditions.

Assessing the Fraud Risk Management Program

Central to providing organizationwide assurance on fraud risk is internal audit's assessment of each component of the fraud risk management program. Utilizing the COSO *Fraud Risk Management Guide* as an appropriate structure, Figure 4 shows questions for the internal auditor to consider.

Figure 4: Assessing the Fraud Risk Management Program

Control Framework	Fraud Risk Management Principles: Questions for Internal Auditors
1. Control Environment	• Does the organization use an enterprisewide risk management or other framework for its fraud risk management program? • Has the organization adopted all components of a fraud risk management framework? • Are there clearly defined roles and responsibilities for fraud risk management at every level? • Do managers and employees understand their roles and responsibilities for antifraud controls? • What elements of the internal and external environments create pressure on fraud risk management and may be a source of new and emerging fraud risks? This may include: o New or changed regulatory requirements. o Changes to organizational structure, reporting lines, and responsibilities. o Expansion into new markets and geographical regions. o Disruption within the sector and industry. o Disruption to third party vendors, agents, distributors, and supply lines. o Changes to compensation model for managers. • Is there a code of ethics and conduct, fraud risk management or fraud control policy, and investigation guidelines in place? • Do fraud, waste, and abuse guidelines exist? • Are fraud policies and procedures clear and comprehensive? • Are fraud policies and procedures accessible to all employees and, where appropriate, in local languages? • Are senior managers and members of the board familiar with their responsibilities for fraud risk governance and management? • Is there a confidential reporting process for whistleblowers? • Are antifraud standards and policies acknowledged and followed by senior management and the board? • Are management's style and behavior consistent with an antifraud culture? • Is there a clear commitment to transparency, integrity, and ethical behavior?
2. Risk Assessment	Do the processes and methods for identifying and assessing fraud risk consider potential sources of: • Incentives or pressure employees may be exposed to (for example, staffing shortages, tight deadlines, reorganization, new or additional responsibilities, challenging performance measures, internal competition, and strict models for compensation and recognition)? • New opportunities for fraud (for example, changes to structures, responsibilities, or control activities)? • Rationalization for fraud (for example, demotion, reduced compensation, external societal or economic pressures)?
3. Control Activities	• Do managers possess the necessary skills and resources to implement control activities effectively and consistently? • Are there regular opportunities for maintaining and increasing fraud risk awareness among all staff together with training as required? • Is the code of conduct communicated, enforced, monitored, and routinely updated? • Does the organization promote training, education, and competence about fraud risks at all levels? • Are antifraud measures consistently enforced in accordance with policies and procedures? • Are those authorized and responsible for managing fraud risks held accountable? • Are employees required to sign in acknowledgement of reading the code of conduct and fraud policies? • Are all employees required to undertake fraud awareness training regularly? • Is the training relevant, robust, and effective? • Does the organization deploy a variety of methods for delivering antifraud training and awareness?

4. Information and Communication	• Are fraud risk governance and management roles and responsibilities clearly documented, communicated, and kept up to date? • Are weaknesses in antifraud controls addressed promptly once they have been identified? • Is the process to obtain, retain, and treat reported concerns and complaints documented? • Are reporting mechanisms (hotline, website, mobile app, etc.) appropriately resourced and are issues duly escalated and evaluated? • Are investigations performed in accordance with protocols approved and documented by the board of directors? • Are personnel assigned to conduct investigations free from conflicts of interest? • Does the board of directors have the ability to obtain outside experts and legal counsel when conducting an investigation? • Do investigators perform root cause analysis as part of the investigation process? • Are weaknesses in antifraud controls investigated and addressed? • Are investigation findings reported to the board of directors in a timely manner and shared with external auditors as needed? • Are disciplinary actions taken against perpetrators of fraud consistently applied regardless of position within the organization? • Are performance metrics used to periodically evaluate the investigation process?
5. Monitoring Activities	• How are lessons learned embedded or taken into account in the revision of controls, policies, and procedures? • Are automated monitoring and continuous auditing processes in operation? • Do fraud risk management monitoring plans focus on objectives with the highest levels of fraud risk? • Does the organization's fraud risk management framework provide sufficient criteria for evaluation? • Do the monitoring activities include consideration of related third parties (joint ventures, foundations, programs funded by the organization, etc.)? • Are antifraud controls monitored regularly by those accountable? • Do members of management participate in routine and ad hoc monitoring and assessment? • Are deficiencies identified in the fraud risk management program reported to the board of directors and remediated on a timely basis? • Is there sufficient coordination and cooperation among assurance providers and management to ensure effective and efficient coverage of fraud risk?

Reporting Assurance on Organizationwide Fraud Risk Management to Senior Management and the Board

The CAE must communicate any significant fraud risk, control, and governance issue periodically to senior management and the board. The board and CAE may wish to establish the types of fraud and the level of materiality or significance that should be reported and a protocol for escalations. It may be appropriate for the CAE to discuss factors related to culture and the control environment that create pressures or opportunities to perpetrate a fraud. The CAE should also provide updates regarding the status of suspected frauds previously reported and any ongoing investigations. The CAE is responsible for assuring the board that management has accepted a level of risk consistent with the board's fraud risk appetite. The CAE must try to resolve the situation with management if exposure to fraud risk is greater than the appetite, and if this remains unresolved, the CAE should notify the board.

In presenting conclusions and a report to senior management and the board, the CAE should address the following questions:

- Is fraud risk management comprehensive, continuous, and aligned with strategic objectives?
- Is the fraud risk management program documented and supported by an organizationwide level of awareness?

- Are arrangements for governance of fraud risk management adequate and effective, including an antifraud culture led by senior management and the board?
- Does management possess the necessary skills, resources, and inclination to provide effective fraud risk management?
- Did management cooperate with the assessment or was there any resistance?
- Are there any significant residual fraud risks?
- Has management accepted a level of fraud that is consistent with the board's risk appetite and the objectives of the organization? If not and the CAE has been unable to resolve the matter, has it been communicated to the board?

Appendix A. Related IIA Standards and Guidance

The following IIA resources were referenced throughout this practice guide. For more information about applying the *International Standards for the Professional Practice of Internal Auditing*, please refer to The IIA's Implementation Guides.

Code of Ethics
Principle 1: Integrity
Principle 2: Objectivity
Principle 3: Confidentiality
Principle 4: Competency
Standards
Standard 1000 – Purpose, Authority, and Responsibility
Standard 1100 – Independence and Objectivity
Standard 1110 – Organizational Independence
Standard 1112 – Chief Audit Executive Roles Beyond Internal Auditing
Standard 1120 – Individual Objectivity
Standard 1130 – Impairment to Independence and Objectivity
Standard 1200 – Proficiency and Due Professional Care
Standard 1210 – Proficiency
Standard 1220 – Due Professional Care
Standard 2050 – Coordination and Reliance
Standard 2060 – Reporting to Senior Management and the Board
Standard 2120 – Risk Management
Standard 2210 – Engagement Objectives
Guidance and Other IIA Resources
Practice Guide "Auditing Anti-corruption Activities," 2021.
Practice Guide "Engagement Planning: Assessing Fraud Risks," 2017.
Position Paper "Fraud and Internal Audit: Assurance Over Fraud Controls Fundamental to Success," 2019.
Position Paper "Three Lines Model," 2020.

Appendix B. Glossary

Definitions of terms marked with an asterisk are taken from the "Glossary" contained in The IIA's publication, *"International Professional Practices Framework*®, 2017 Edition" (also known as the Red Book), published by the Internal Audit Foundation. Other sources are identified in footnotes.

board* – The highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, "board" in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

chief audit executive* – Describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.

conflict of interest* – Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.

control* – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

corruption – The use of power, money, or favors by people in positions of authority or contacts in their network for illegitimate private gain.[3]

fraud* – Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

[3] The IIA's Practice Guide "Auditing Anti-corruption Activities," 2021. https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/auditing-anti-corruption-activities/.

governance* — The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

impairment* — Impairment to organizational independence and individual objectivity may include personal conflict of interest, scope of limitations, restrictions on access to records, personnel, and properties, and resource limitations (funding).

independence* — The freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner.

objectivity* — An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others.

professional skepticism — An inquisitive attitude, free of bias or assumptions about the inherent honesty of management or employees.[4]

risk appetite* — The level of risk that an organization is willing to accept.

[4] The IIA's Practice Guide "Engagement Planning: Assessing Fraud Risks," 2017. https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/engagement-planning-assessing-fraud-risks/.

Appendix C. References and Additional Reading

References

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrating Strategy and Performance*, 2017. https://www.theiia.org/en/products/bookstore/coso-enterprise-risk-management-integrating-with-strategy-and-performance/.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Fraud Risk Management Guide*, 2016. https://www.theiia.org/en/products/bookstore/fraud-risk-management-guide/.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control – Integrated Framework*, 2013. https://www.theiia.org/en/products/bookstore/coso-internal-control-integrated-framework-2013-framework/.

Cressey, Donald R. "Other People's Money: A Study in the Social Psychology of Embezzlement, (Glencoe, IL Free Press, 1953)

The IIA, *International Professional Practices Framework*, 2017. https://www.theiia.org/en/standards/.

Additional Reading

"Antifraud Collaboration: Skepticism in Practice," AFC Anti-Fraud Collaboration, 2020. https://www.theiia.org/globalassets/documents/news/press-releases/2020/september/afc-skepticism-in-practice.pdf.

Fountain, Lynn. *Raise the Red Flag: An Internal Auditor's Guide to Detect and Prevent Fraud.* Altamonte Springs, FL: The IIA Research Foundation, 2015. https://www.theiia.org/en/products/bookstore/coso-enterprise-risk-management-integrating-with-strategy-and-performance/.

"Report to the Nations," ACFE, 2020. https://www.thirdline.io/blog/acfe-post#:~:text=The%20Report%20to%20the%20Nations%20is%20a%20global,5%25%20of%20their%20revenue%20to%20fraud%20each%20year.

Rittenberg, Larry. *COSO Internal Control – Integrated Framework: Turning Principles into Positive Action*. Altamonte Springs, FL: The IIA Research Foundation, 2013. https://www.theiia.org/en/products/bookstore/coso-internal-control-integrated-framework-turning-principles-into-positive-action/.

Tosh, Steve, "12 Key Factors to Support Transformation Into an Anti-Fraud Culture," Global Risk Alliance, 2021. https://www.global-riskalliance.com/post/anti-fraud-culture.

Acknowledgements

Guidance Development Team

Hans-Peter Lerchner, CIA, CRMA, Austria (Project Lead)
Tuncay Efendioglu CIA, CCSA, CFSA, CRMA, Canada
James T. Enstrom, CIA, USA
Charlotta Lofstrand Hjelm, CIA, QIAL, Sweden
Stavri Pashko, CIA, Sweden
Jason Robert Thogmartin, CIA, CRMA, USA

Guidance Contributors

David Dominguez, CIA, CRMA, USA
Michael Dorn, CIA, CRMA, USA
Francesca Gabella, CRMA, UK
Nikolaus Rechnitzer, CFE, Austria
Astra Williamson, Canada

Global Guidance Council Reviewers

Susan Haseley, CIA, USA
Lesedi Lesetedi, CIA, QIAL, CRMA, Botswana
Karem Obeid, CCSA, UAE
Klaus Rapp CIA, Switzerland
Tichaona Zororo, CIA, CRMA, South Africa

International Internal Audit Standards Board Reviewers

Stephen Coates, CIA, CGAP, CRMA, Australia
Naji Fayad, CIA, CCSA, CRMA, Saudi Arabia

IIA Global Standards and Professional Practices

Dr. Lily Bi, CIA, QIAL, CRMA, CISA, Executive Vice President
Anne Mercer, CIA, CFSA, CFE, Senior Director (Project Lead)
Shelli Browning, Associate Manager
Helen Nicholson, Content Writer and Technical Editor

The IIA thanks the following oversight bodies for their support: Global Guidance Council, International Internal Audit Standards Board, and the International Professional Practices Framework Oversight Council.

About The IIA

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 210,000 members and has awarded 180,000 Certified Internal Auditor (CIA) designations worldwide. The IIA is recognized as the internal audit profession's leader in standards, certification, advocacy, education, research, and technical guidance throughout the world. The IIA's global headquarters is located in Lake Mary, Fla. For more information, visit www.theiia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

May 2022

The Institute of
Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101